Shortfalls related to the security of the Project 25 (P25) standard identified last year generally can be resolved through sound operational and information security procedures.

By Bill Pagones

Discussion about security surrounding LMR, particularly shortfalls of the Project 25 (P25) standard related to security, have become commonplace. The problems identified are not limited to the P25 technologies, but affect wireless communications as a whole. While some of the issues identified are technical in nature, the vast majority can be resolved through sound operational and information security procedures.

Members of the Project Technology 25 Interest Group (PTIG), an organization of users and manufacturers of P25 systems, have significant experience in how P25 radios are designed and encrypted. PTIG recognizes the inherent weaknesses in any radio system, but also strives, in concert with the Telecommunications Industry Association (TIA) and the Project 25 Steering Committee, to address those weaknesses and decrease the risks involved.

No radio transmission, however protected or encrypted, is totally immune to selective attacks. The best we can hope for is to protect the radio from these attacks by following best practices and to encrypt radio transmissions to the highest level possible, consistent with the sensitivity of the information being protected.

P25, published as a suite of TIA-102 standards, is a global standard for public safety and critical communications for LMR. Arguably, it's the most robust digital standard for public-safety grade radios in the world, and the predominant standard in North America. From a security perspective, the P25 standard enables the ability to securely transmit sensitive information among the users of a system. The degree of encryption, such as the algorithm strength and complexity of the key, is the means of protection. Encryption for public-safety grade radios can range from simple scrambling to complex 256-bit key advanced encryption.

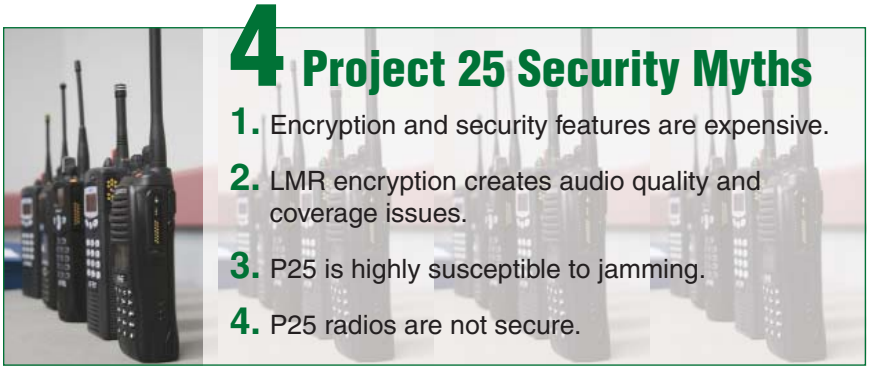
The P25 suite of standards adopted 256-bit advanced encryption standard (AES) as its choice for securing, to a high degree, radio traffic that must be protected. The P25 Block Encryption Protocol (TIA-102.AAAD-A) also allows the use of the data encryption standard-output feedback (DES-OFB) and triple encrypted DES (3DES). A large number of U.S. users still operate DES-OFB. As a result, many agencies operate both DES-OFB and AES to allow encrypted interoperability options for their agents in the field. The federal government strongly recommends all public-safety agencies migrate to AES for increased message security.

With any technology there can be misunderstandings, based on certain assumptions that can be construed as vulnerabilities or weaknesses in the use of the technology. In this regard, P25 radio systems are no different. It's obvious that public-safety communications are specifically designed to provide highly reliable communications. In some cases a radio is the only lifeline an officer has available. An agency might want to protect specific information, but in an emergency situation, the ability to talk unencumbered may overcome the need to protect the information. The relative vulnerability of P25 radios to jamming or eavesdropping depends partially on what assumptions are made when exposing its weaknesses.

This topic has been discussed a great deal in recent studies and in recently published articles. This article will detail some of the key myths that have led to misunderstandings about P25 and how it behaves, and offers the facts. These facts may calm some of the artificially created uncertainty and uneasiness about the performance of P25 systems in the public-safety radio marketplace.

Myth No. 1:
Encryption and Security Features Are Expensive

Not long ago, the cost of encryption was almost as expensive as the radio itself, not to mention the extra equipment required to rekey the



4 Project 25 Security Myths

1. Encryption and security features are expensive.
2. LMR encryption creates audio quality and coverage issues.
3. P25 is highly susceptible to jamming.
4. P25 radios are not secure.

radios. With current radios, the cost to include encryption is a fraction of the total cost associated with the radio. Some vendors have inexpensive solutions to implement standardized encryption algorithms as part of their product offerings. Other vendors provide encryption choices at various cost levels, but even the highest price option is significantly less than early implementations of encrypted LMR.

While the cost of encryption for radios has decreased, the infrastructure necessary to support encryption and other security features remains fairly expensive. Even though the infrastructure is expensive, the return on investment (ROI) is fairly quick. One example is over-the-air-rekeying (OTAR), the ability to rekey an entire radio fleet without having to manually and physically update every radio. The use of OTAR could offset the cost of the necessary additional infrastructure with significant reduction in resources, such as manpower, which could be used elsewhere.

Although there is not a monetary value readily available, encryption and security services provide improved officer safety and mission integrity by protecting critical information. Clear transmissions have been shown to alert suspects of pending raids and other time-sensitive information.

Myth No. 2:
Encryption Creates Audio Quality and Coverage Issues

When analog was dominant, cipher feedback encryption could cause significant coverage loss — as much as 3 dB loss — and could degrade audio quality. With the advent of digital LMR and the output feedback algorithms used by both DES and AES, coverage and voice quality are no longer an issue because of encryption. All encryption is done after the voice is processed by the vocoder, and encryption is a digital packet stream, having no impact on audio quality and not introducing any degradation of range or signal quality. Unfortunately, the earlier shortcomings forced some public-safety agencies to adopt operational policies that dictated unencrypted transmissions. Because of this myth, many of these operational policies have not been updated for digital implementations.

Myth No. 3:
P25 is Highly Susceptible to Jamming

All wireless communications are susceptible to jamming. Public-safety agencies deal with unintentional jamming regularly. The act of selective or intentional jamming is far more problematic for system administrators. The source of the jamming is often not known and may not be regularly interfering with the communications system. In most cases, mitigation solutions are available to deal with the interference. As the interference increases in complexity, the mitigation strategy and solution increases in complexity and cost. While a number of articles discuss the use of commercial-off-the-shelf (COTS) products to jam public-safety communications, in almost every case, these incidents are highly localized and require significant modifications to the COTS product.

Myth No. 4:
P25 Radios Are Not Secure

P25 was designed as a public-safety-grade interoperable communications standard. Encryption and security services were added, as an option, for agencies requiring secure communications. Security services that include encryption and the choice to use them are solely policy and operational decisions made by the jurisdiction or agency implementing the communications system.

The P25 suite of standards includes more than half a dozen standards specifically focused on security services. These services include encryption, key fill device interfaces, OTAR, key management facility (KMF), and key fill device protocols and link layer authentication. The P25 Steering Committee, in cooperation with TIA, the National Institute for Standards and Technology (NIST), and Institute for Telecommunication Sciences (ITS), is continually identifying and drafting new standards to further the security services portfolio. Additionally, the published standards are reviewed and updated regularly to correct discrepancies, oversights and issues related to interoperability. Several items to address message authentication, replay protection, KMF-to-KMF key sharing and link layer encryption are in development.

The Block Encryption Protocol document specifically addresses how DES, 3DES and AES should be implemented for P25. Originally the document was developed and published when DES was the primary federal standard for encryption. However, NIST withdrew DES and recognized AES as the only approved algorithm for use by federal agencies. It is notable that none of the security vulnerability studies and published articles that stimulated this discussion has shown evidence of being able to compromise the AES key.

The Federal Partnership for Interoperable Communications (FPIC) recognized a large number of DES implementations are still active in the public-safety community.

Acknowledging the fact that a vast number of other protection algorithms are available, FPIC also recommended that agencies implement the AES 256-bit algorithms and retain DES only where needed for interoperability purposes. The FPIC encouraged agencies to migrate to the more secure AES algorithm as soon as possible. The DES algorithm is increasingly more susceptible to brute-force exhaustive key search attacks. The P25 Steering Committee, in coordination with the P25 User Needs Subcommittee, adopted the FPIC recommendation to make the 256-bit AES algorithm the primary encryption method as published in the P25 statement of requirements (SoR) dated April 8, 2011.

"There is nothing inherent in P25 that makes this problem any worse than in any other communications system (including analog)," said John Oblak, chair of the TIA TR-8 private LMR systems engineering committee. PTIG members will continue to educate the community on how the P25 standard improves public-safety communications. PTIG members, TIA and the P25 Steering Committee work together to continuously update all aspects of the standard to enhance its performance and mitigate security vulnerabilities.

In so many ways, P25 is a vast improvement over what public-safety agencies used not so long ago and that some still use. P25 improvements serve not only total system functionality, but also improve the ability to protect mission-critical information. Many U.S. public-safety agencies are leveraging P25 to help address the technical, operational and economic challenges faced in the communications environment. Benefits realized through the use of the P25 standard include not only improved security, but improved interoperability across jurisdictions and levels of government, enhanced spectral efficiency, increased competition among vendors and backward compatibility to allow graceful migration to new technologies. ■

Basil (Bill) Pagones is the executive director of the Project 25 Technology Interest Group (PTIG). Visit www.project25.org for more information. Email comments to editor@RRMediaGroup.com.

RadioResource *MissionCritical Communications* delivers wireless voice and data solutions for mobile and remote mission-critical operations. The magazine covers business, public safety, and regulatory news; case studies; in-depth features; innovative applications; product information and comparisons; emerging technologies; industry reports and trends; and technical tips. In addition, each issue contains *Public Safety Technology*, a special section devoted solely to the needs of the public safety community. Editorial content targets organizations in the United States and Canada with mobile and remote communications needs, including public safety, government, transportation, manufacturing, utility/energy, business, and industrial entities. To request a FREE subscription or get more information, go to www.mccmag.com. RadioResource *MissionCritical Communications* is published by the RadioResource Media Group. Pandata Corp., 7108 S. Alton Way, Building H, Centennial, CO 80112, Tel: 303-792-2390, Fax: 303-792-2391, www.rrmediagroup.com. Copyright 2012 Pandata Corp. All rights reserved. Reprinted from the February 2012 issue of RadioResource *MissionCritical Communications*. For more information about *MissionCritical Communications* and the RadioResource Media Group please call 303-792-2390 or visit www.mccmag.com